POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS FUNCIONÁRIOS DA ASSOCIAÇÃO CONGREGAÇÃO DE SANTA CATARINA – COOPERCREDI ACSC

DAS DEFINIÇÕES

1. Visa prover diretrizes para a segurança da informação, relacionadas ao manuseio, controle, proteção (contra indisponibilidade, divulgação imprópria, acesso indevido e modificação não autorizada de informações e de dados) e descarte;
2. É elaborada pela Diretoria Executiva, com apoio das áreas subordinadas.
3. Deve ser revisada no mínimo anualmente ou a qualquer tempo em decorrência de fatos relevantes, bem como por orientação ou normatização expedida pelo Sicoob e órgãos reguladores.
4. É observada por todos os usuários que compõem as estruturas organizacionais (dirigentes, empregados e estagiários) da Coopercredi ACSC e pelas demais pessoas com acesso autorizado às informações da Cooperativa;
5. Preservar as informações da Coopercredi ACSC quanto à:
    a. **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
    b. **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
    c. **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
6. Todo e qualquer usuário de recursos computadorizados da Coopercredi ACSC tem a responsabilidade de proteger a segurança e a integridade das informações, da infraestrutura e dos equipamentos de tecnologia. A violação desta política de segurança é qualquer ato que:
    a. Expõe a Coopercredi ACSC a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados, da rede lógica, das informações ou ainda da perda de equipamento;
    b. Envolva a revelação de dados confidenciais, direitos autorais, negociações a disponibilização, cópia e uso não autorizado de dados corporativos;
    c. Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

DO OBJETIVO

7. O objetivo da Política de Segurança da Informação é garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a oferta de produtos, prestação de serviços e continuidade dos negócios da Coopercredi ACSC.

DA MISSÃO DA UNIDADE ADMINISTRATIVA

8. Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da Coopercredi ACSC. Ser o gestor do processo de segurança e proteger as informações da organização, monitorando, coordenando, suportando, desenvolvendo e/ou implementando ações para esta finalidade.
9. A Unidade Administrativa, com autorização da Diretoria Executiva poderá contratar terceiros para auxiliar na execução desses serviços.

DA GESTÃO DA INFORMAÇÃO

10. Todos os usuários da Coopercredi ACSC devem considerar a informação como sendo o maior bem da organização. A informação é um dos recursos críticos para a realização do negócio, que possui grande valor para a empresa e deve sempre ser tratada, conduzida e transmitida de forma profissional.

11. É de responsabilidade dos diretores, gestores e superintendentes estabelecer critérios do nível de confidencialidade das informações (relatórios e/ou mídias) geradas pelas áreas classificando as informações de acordo com a tabela abaixo:
    a. **Informação pública:** é toda informação que pode ser acessada por usuários da Coopercredi ACSC, clientes internos e externos, fornecedores, prestadores de serviços e público em geral.
    b. **Informação interna:** é toda informação que só pode ser acessada pelos colaboradores da empresa. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
    c. **Informação confidencial:** é toda informação que pode ser acessada somente por determinados usuários do da Coopercredi ACSC, gestores, superintendentes, diretores e conselheiros. A divulgação não autorizada dessa informação pode causar risco financeiro, de imagem ou operacional ao negócio do da Coopercredi ACSC
    d. **Informação restrita:** é toda informação que pode ser acessada somente por grupo de usuários da empresa, previamente definidos. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Os gestores e superintendentes devem orientar seus subordinados a não circularem informações, arquivos ou mídias consideradas confidenciais ou restritas, como também não deixar relatórios nas impressoras, mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.
    e. **Conversação:** é toda a informação proferida entre os colaboradores através de sistemas de conversação, com o intuito de agilizar o atendimento, reduzir custo e viabilizar processos.

DOS DADOS DOS FUNCIONÁRIOS

12. A Coopercredi ACSC se compromete a não acumular ou manter intencionalmente dados pessoais de funcionários, além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de funcionários que porventura sejam armazenados serão considerados dados confidenciais e não utilizados para fins diferentes daqueles para os quais foram coletados.
13. Dados pessoais de funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários no domínio crediacsc.org.br. Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da empresa, sem prévia e expressa autorização por parte da Diretoria Executiva.
14. Mesmo que seja autorizado o armazenamento destes dados, a empresa não se responsabiliza por eles, nem tão pouco pelo seu conteúdo e segurança. Tais dados jamais poderão ser armazenados nos diretórios dos servidores de empresa, e não farão parte da rotina de backup da empresa.

DA ADMISSÃO E DEMISSÃO DE COLABORADORES

15. A Unidade Administrativa tem por obrigação informar formalmente e com antecedência de 1 a 3 dias úteis a admissão, demissão e afastamento de colaboradores, estagiários e terceiros a área responsável, para que sejam realizados os procedimentos necessários relativos a disponibilização ou não de recursos de infraestrutura e acesso às informações. Neste processo a Unidade Administrativa é responsável pela liberação de usuário e senha para acesso à rede lógica e para uso dos recursos de telefonia.
16. Nos casos de admissão de colaboradores, a Unidade Administrativa deverá informar a área e unidade em que o mesmo será admitido, visando estabelecer o perfil correto de acesso na rede lógica.
17. Nos casos de demissão, o RH deverá comunicar o fato o mais rápido possível à Unidade Administrativa, para que sejam bloqueadas senhas de acesso à rede lógica e de telefonia.
18. Caso o colaborador necessite copiar alguma informação pessoal da sua estação de trabalho, caberá ao gestor autorizar e acompanhar o processo para que não haja extravio de informações pertinentes a Coopercredi ACSC.
19. Na admissão de colaboradores, cabe ao RH divulgar e colher assinaturas do colaborador sobre concordância aos procedimentos estabelecidos na Política de Segurança da Informação do Coopercredi ACSC. Nenhum colaborador, estagiário ou temporário poderá ser contratado, sem ter expressamente concordado com esta política.
20. Na demissão cabe ao RH dar conhecimento e obter as devidas assinaturas do Termo de Confidencialidade, informando ao ex-colaborador sobre as sanções que poderão ser realizadas caso seja identificada divulgação de informações relativas ao negócio do Coopercredi ACSC, independente da forma em que o mesmo ocorreu.
21. As informações fornecidas pelo RH relativas à admissão, afastamento ou demissão de colaboradores deverão ser realizadas através de formulário F022 - Usuário e acesso, sendo o mesmo classificado com "chamado interno" e tendo prazo de atendimento entre 1 a 3 dias úteis.

DA TRANSFERÊNCIA DE FUNCIONÁRIOS

22. Quando ocorrerem promoções ou transferência de colaboradores de áreas e/ou unidades, o RH deverá informar previamente a Unidade Administrativa para que sejam realizadas as adequações necessárias de perfil de acesso na rede lógica.
23. A informação deverá ser enviada através de email/processo no fluig, e tendo prazo de atendimento entre 3 a 5 dias úteis.

DA INSTALAÇÃO DE PROGRAMAS

24. Atendendo à determinação legal, a Coopercredi ACSC respeita os direitos autorais dos softwares e aplicativos utilizados e instalados nos servidores, estações de trabalho e notebooks para uso exclusivo dos clientes internos e fornecedores devidamente registrados para trabalhos pontuais, autorizados pelo gestor da área contratada. Portanto, todo e qualquer software, aplicativo ou ferramenta deverá ser homologado e adquirido pelo Administrativo, pagando o real valor por licença utilizada e isentando a Coopercredi ACSC de qualquer penalidade referente ao uso de software ilegal.
25. É responsabilidade somente da Unidade Administrativa, realizar a instalação e configuração do software nos servidores, estações de trabalho e notebooks, assegurando que todas as licenças estão devidamente legalizadas e a ferramenta estará disponível somente aos usuários com esse perfil de uso.
26. É proibida a instalação de softwares, aplicativos e ferramentas por qualquer outro colaborador que não seja da equipe da Unidade Administrativa. Periodicamente e sem aviso prévio, o administrativo fará verificações nos servidores, estações de trabalho e notebooks dos colaboradores, visando garantir a correta aplicação desta diretriz. Caso

sejam encontrados programas não autorizados estes serão removidos e será comunicado o gestor da área.

27. Caso a instalação do software não licenciado acarrete em perda de informação, exposição à fraude ou multa, o colaborador poderá ser penalizado pelo custo desembolsado pela Coopercredi ACSC.
28. A Diretoria poderá utilizar de sua autonomia para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à lei do software (Lei 9.609/98).

DAS PERMISSÕES E SENHAS

29. Todos os usuários da rede lógica, de sistemas e de telefonia deverão possuir um usuário e senha previamente cadastrados pelo administrativo. Ela fornecerá uma senha padrão ao colaborador, que deverá efetuar a troca no primeiro acesso na rede.
30. A Coopercredi ACSC utiliza um critério de segurança para a criação de senhas. Portanto, todas as senhas deverão conter letras maiúsculas, minúsculas, números e caracteres especiais (!,@,#,$%,&,*). As senhas devem conter no mínimo seis e no máximo oito caracteres.
31. Será solicitada a troca de senha à todos os usuários a cada 90 dias, não podendo ser utilizadas as últimas três senhas anteriores.
32. O usuário que digitar a senha errada por seis vezes, terá seu acesso bloqueado automaticamente pelo sistema por questões de segurança. É uma medida básica para evitar violações no acesso local, quando alguém está diante do computador sem acesso autorizado.
33. O cadastro de senhas de rede lógica e telefonia é realizada exclusivamente pela administrativo, por usuários com perfil de administrador de domínio (domain admin). Caso o usuário esqueça a senha deverá se dirigir ao administrativo que atribuirá e informará novamente uma senha padrão, solicitando a troca no primeiro acesso.
34. A inclusão de novos usuários, com senha e perfil determinado será realizada somente mediante formulário.
35. No caso de disponibilização de senha para terceiro, prestador de serviço ou órgão fiscalizador, o formulário deverá ser entregue constando assinatura do gestor da área ou da diretoria. Caberá à área demandante também informar o bloqueio do usuário e senha, tão logo esteja concluído o trabalho para que a mesma não seja utilizada indevidamente.
36. No caso da contratação de gestores, assessores com perfil e alçada de procurador da Coopercredi ACSC, permitindo a aprovação de documentos e valores através do sistema de bancos, essa característica deverá ser destacada no formulário.

DO COMPARTILHAMENTO DE DADOS

37. Não é permitido o compartilhamento de informações, dados e pastas nas estações de trabalho e notebooks. Portanto, todas as informações pertinentes aos produtos e serviços prestados, bem como às regras de negócio da Coopercredi ACSC, deverão ser armazenados preferencialmente no Google Drive e compartilhado de acordo com as obrigações de cada colaborador e nos servidores de rede.
38. O acesso das informações será garantido com a definição do perfil de cada usuário na sua inclusão. Portanto, cada colaborador terá acesso somente às informações que lhe convierem.
39. A Coopercredi ACSC possui somente três senhas com perfil de administrador de domínio (domain admin) que permitem que o colaborador através de acesso à rede lógica possa visualizar todas as informações constantes em todas as pastas disponíveis nos servidores de rede e pelo perfil definido no Google Drive para poder visualizar as pastas que lhe convier. Contudo, os acessos destes colaboradores são monitorados.

40. Todos os demais colaboradores, mesmo os da administrativo, estão inseridos com o perfil de usuário comum seguindo os critérios de acesso restritos ao seu perfil.
41. Nos servidores de rede, há o seguinte critério de pastas e arquivos disponível a todos os usuários:
    a. A unidade W: contem pasta para cada área, sendo as seguintes estruturas macros, que podem ser alteradas conforme avaliação da Unidade Administrativa:
        i. Área de Relacionamento com o Cooperado;
        ii. Controladoria;
        iii. Área de Suporte Organizacional;
        iv. Área Operacional
    b. Os usuários têm acesso às pastas da sua área e as compartilhadas com todos os colaboradores;
    c. A Unidade X:\ contém informações de visualização para cada colaborador. Cada colaborador possui a sua pasta e cabe ao proprietário da informação, efetuar a gravação e exclusão de arquivos, bem como atentar ao sigilo e confidencialidade das informações;
42. É de responsabilidade da Coopercredi ACSC, realizar a cópia de segurança (backup) e restauração de informações de todas as unidades. O objetivo é evitar o envio de arquivos por email, que consomem banda de internet tanto no envio como no retorno.
43. O objetivo é permitir que o colaborador possa guardar documentos ou informações na rede ou compartilhar através do Google Drive ao invés de gravar no computador local onde pode correr o risco de perde-las caso o equipamento falhe e fique inutilizado.
44. É importante ressaltar que não são realizadas cópias de segurança (backup) no computador local. Cabe ao proprietário da informação garantir a gravação da informação em local seguro. Portanto, a Coopercredi ACSC não se responsabilizará por quaisquer informações armazenadas e excluídas do computador local e suas subpastas.

DO BACKUP (CÓPIA DE SEGURANÇA DOS DADOS)

45. É de responsabilidade da Unidade Administrativa realizar diariamente as cópias de segurança das informações nos servidores de rede, exceto nos computadores locais
46. O procedimento backup de segurança prevê a realização de um backup por dia sendo feito através de cópia em outros servidores criados na nuvem e também registro no HD externo reservado apenas para backup que se encontra junto ao servidor físico na sede da Cooperativa.
47. Esse processo é feito em um ciclo de regravação.
48. O processo de validação do backup é realizado mensalmente, sempre na 1ª quinta-feira do mês, por determinados profissionais da Unidade Administrativa e terceiros responsáveis pelo processo de backup, sendo restaurada uma pasta aleatória. Este procedimento deverá ser formalizado e assinado pelo gestor da Unidade Administrativa ou na ausência deste por um diretor, atestando que o processo foi realizado de forma adequada.

DAS CÓPIAS DE SEGURANÇA DE ARQUIVOS EM OUTROS MEIOS DE ARMAZENAMENTO

49. Não está contemplado nesta política e não é responsabilidade da Coopercredi ACSC o backup de informações, dados e arquivos dispostos nas estações de trabalho, notebooks e pen-drives.
50. Caso o usuário tenha algum programa que efetue gravação em unidades locais, esse fato deverá ser informado na implantação do sistema, prevendo um procedimento de backup, de forma a armazenar as informações nos servidores de rede.

51. O backup de informações, dados e arquivos armazenados em meios externos são de responsabilidade dos próprios usuários proprietários determinando procedimentos constantes de cópia, garantindo a segurança das informações e continuidade do negócio. Neste caso, havendo perda das informações, o usuário será responsável pela sua recuperação.
52. Portanto, todas as informações consideradas de fundamental importância para a continuidade dos negócios da Coopercredi ACSC deverão ser armazenadas nos servidores de rede e no Google Drive.

DA SEGURANÇA E INTEGRIDADE DOS DADOS

53. A instalação, configuração e gerenciamento do banco de dados é de responsabilidade exclusiva da Unidade Administrativa, assim como a manutenção, alteração e atualização de equipamentos e programas. Entretanto, nos casos de sistemas de terceiros que utilizem o banco de dados, o contrato de manutenção com o fornecedor do mesmo deverá destinar horas para a utilização de profissional com perfil na administração de banco de dados (Database Administrator – DBA), considerando que a Unidade Administrativa não dispõe de profissional com essa qualificação. Não havendo o contrato e identificando a necessidade deste tipo de profissional, o gestor da área proprietária do sistema será responsável por solicitar aprovação de contratação deste profissional.

DA PROPRIEDADE INTELECTUAL

54. É de propriedade da Coopercredi ACSC, todos os "designs", criações, códigos fontes, licenças, executável ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a empresa.
55. O acesso à internet é liberado a todos os colaboradores e usuários da rede lógica. Contudo, o software de controle de conteúdo de Internet realiza um monitoramento de acesso aos sites, realizando a restrição e bloqueio do acesso.
56. Nesse filtro está contemplado a liberação e/ou bloqueios de sites conforme as características da Coopercredi ACSC.
57. O uso da Internet será monitorado pelo administrativo, inclusive através de "logs" (arquivos gerados no servidor) que informam a data, usuário logado, o tempo de uso e a página acessada.
58. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. É terminantemente proibido o acesso, a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites de:
    a. Estações de rádio e TV, etc;
    b. Conteúdo pornográfico ou relacionados a sexo;
    c. Defesa de atividades ilegais;
    d. Preconceito a determinadas classes, raças, etc;
    e. Salas de discussão, blogs pessoais e "bate-papo" que não estejam relacionados aos negócios da Coopercredi ACSC;
    f. Que promovam discussão pública sobre os negócios da Coopercredi ACSC, a menos que autorizado pela Diretoria Executiva;
    g. Que possibilitem a distribuição de informações de nível "Confidencial";
    h. Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.
59. No caso de bloqueio de site relacionado aos negócios da Coopercredi ACSC, o usuário poderá solicitar o desbloqueio desde que autorizado formalmente pelo gestor da área ou diretor. Neste caso, cabe ao gestor realizar o monitoramento de acesso e uso dos sites por ele liberados. Durante o monitoramento realizado pela Unidade Administrativa, os

relatórios de abusos e acessos indevidos a sites serão encaminhados aos gestores de áreas.

DO USO DO CORREIO ELETRÔNICO (E-MAIL)

60. O correio eletrônico fornecido pelo Coopercredi ACSC é um instrumento de comunicação interna e externa para a realização dos negócios e prestação de serviços pelas áreas da empresa.
61. As mensagens devem ser escritas em linguagem profissional, não devem ter palavras de baixo calão ou gírias, de forma a não comprometer a imagem da Coopercredi ACSC. O usuário deve se atentar para as orientações do Manual de Instrumentalização Geral (MIG) e às resoluções que tratam o assunto.
62. Todas as informações dispostas e enviadas por e-mail por colaboradores deverão estar de acordo com a legislação e resoluções vigentes, não podendo ser contrárias e essas.
63. Todas as respostas enviadas por e-mail deverão conter a assinatura do colaborador. Em casos específicos, cada área poderá incluir a assinatura do gestor ou do superior imediato no e-mail. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.
64. É terminantemente proibido o envio de mensagens que:
    a. Contenham declarações difamatórias e linguagem ofensiva;
    b. Possam trazer prejuízos a outras pessoas;
    c. Sejam hostis e inúteis, contenham palavras de baixo calão;
    d. Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;
    e. Possam prejudicar a imagem da organização;
    f. Possam prejudicar a imagem de outras empresas;
    g. Sejam incoerentes com as políticas da Coopercredi ACSC.
65. . Para incluir ou remover um usuário no correio eletrônico e/ou grupos departamentais, a área solicitante ou a Unidade Administrativa (novos colaboradores / demissionários) deverá encaminhar pedido formal através de formulário ou email com os dados completos, bem como o objetivo da inclusão. A Unidade Administrativa providenciará a disponibilização dentro do prazo de classificação.
66. A utilização do "e-mail" deve ser criteriosa, evitando envio de anexos maiores que 25 Mb para um grupo de pessoas. Com isso, evitaremos o congestionamento da banda larga que gerará impacto em outras atividades que utilizam esse mesmo recurso de internet, como por exemplo, suporte remoto.
67. No caso de congestionamento no sistema de correio eletrônico o administrativo fará o monitoramento e auditoria no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

DA COMUNICAÇÃO INSTANTÃNEA

68. É permitido apenas o comunicador do email do Google para utilização entre os colaboradores da Coopercredi ACSC, ficando vedado a utilização de outros softwares com características de comunicador instantâneo (Google Talk, MSN, etc), instalados ou não nas estações de trabalho e equipamentos portáteis.

DA NECESSIDADE DE AQUISIÇÃO DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

69. A Coopercredi ACSC é responsável pela aplicação da Política de Segurança da Informação em relação à homologação técnica na compra, upgrade e substituição de software e hardware. Portanto, na aquisição destes itens o administrativo deverá participar realizando estudo de viabilidade das questões tecnológicas para que os novos ativos estejam em consonância com o ambiente atual.

70. Parágrafo único: Não é permitida a compra, desenvolvimento, instalação e implantação de softwares, hardware ou periféricos diretamente pelos usuários, sem a homologação e participação do Administrativo.

DO USO DE EQUIPAMENTOS PORTÁTEIS

71. Os usuários que utilizam equipamentos portáteis como notebooks smartphones, tablet ou qualquer outro equipamento computacional móvel, de propriedade da Coopercredi ACSC devem estar cientes que:
    a. Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais. A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
    b. É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
    c. Não é permitido ao usuário do equipamento realizar alteração de configuração do equipamento recebido, formatação, instalação/remoção de sistema operacional, instalação de softwares.
    d. Na entrega do equipamento seja para uso contínuo ou por tempo determinado, o usuário deverá assinar um termo de responsabilidade pelo equipamento garantindo que o mesmo seja entregue nas mesmas condições em que foi retirado, considerando os aspectos físicos e lógicos, hardware e software, sistema operacional e periféricos que o acompanharem.
72. É imprescindível que os usuários atentem para alguns cuidados básicos que visa garantir a segurança, alta disponibilidade e pleno funcionamento do equipamento:
73. Quando o usuário for utilizar o equipamento fora da empresa, o colaborador
74. Deverá atentar seguir as seguintes regras:
75. Mantenha o equipamento sempre com você;
76. Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.;
77. Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível, mas atente-se para que não fique se deslocando durante a viagem ou prensado entre as bagagens de forma a danificar o equipamento;
78. Atenção ao transportar o equipamento na rua utilize bagagem que não chame a atenção ao furto ou roubo;
79. Se tiver informações importantes armazenadas no notebook, sempre mantenha uma cópia de segurança na empresa;
80. O administrativo poderá disponibilizar uma forma de acesso a rede interna para o transporte das informações e/ou acesso as aplicações da Coopercredi ACSC.
81. Em caso de furto o colaborador deverá atentar as seguintes regras:
    a. Não reaja ao furto;
    b. Registre um boletim de ocorrência em uma delegacia de polícia;
    c. Comunique ao seu superior imediato e a Unidade Administrativa;
    d. Envie uma cópia da ocorrência para a Unidade Administrativa
82. Outras dicas importantes de uso de equipamentos portáteis:
    a. Cuidado com os fios da fonte de energia e do mouse. Não enrole os fios, pois poderão quebrar internamente gerando um curto circuito ou a indisponibilidade de uso do equipamento;
    b. Quando não estiver conectada a rede lógica da Coopercredi ACSC atente para o acesso a sites indevidos, download de arquivos mal-intencionados ou que possam contaminar com vírus o seu notebook e proliferar para toda a rede;
83. Lembramos que esse tipo de equipamento mesmo sendo de uso exclusivo é de propriedade da Coopercredi ACSC, cabe ao seu usuário prover condições que mantenham em pleno funcionamento.

84. A utilização de Modens 3G nas dependências da Coopercredi ACSC, tem que ser autorizada pelo gestor da área em comum acordo com a diretoria. Esta medida visa garantir a segurança dos dados da rede do Unidade Administrativa.

RESPONSABILIADE DOS GESTORES /DIRETORES

85. Os diretores e gerentes são responsáveis pelas definições de perfil de acesso de seus colaboradores, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas atribuições, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.
86. O administrativo fará auditorias periódicas de acesso dos usuários às informações, da rede interna da Coopercredi ACSC.

DOS SISTEMAS DE TELECOMUNICAÇÕES

87. Na admissão do colaborador o mesmo recebe orientações para o uso
88. de acordo com o perfil determinado pelo seu gestor.
89. É proibido aos colaboradores das demais áreas adquirir equipamentos e softwares de telefonia sem a autorização da Coopercredi ACSC.

DO USO DE ANTIVÍRUS

90. Visando garantir a alta disponibilidade, a segurança das informações e a continuidade do negócio da Coopercredi ACSC, todos os servidores, estações de trabalho e notebooks dispõem de software antivírus.
91. Esses sistemas estão permanentemente configurados para detectar possíveis ameaças em todos os arquivos, nos dispositivos e mídias externas.
92. Cabe a todos os usuários zelar pela segurança do seu equipamento e da rede lógica, realizando sempre uma varredura em arquivos abertos no seu equipamento, pen-drives e CD/DVD, bem como atentar na abertura de links que não estejam relacionados com o negócio da Coopercredi disponíveis em sites ou encaminhados por e-mail.
93. . Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por softwares de antivírus.
94. A atualização da lista de vírus é realizada automaticamente pelos servidores, replicando para as estações de trabalho automaticamente.
95. O usuário não pode em hipótese alguma desabilitar o software de antivírus instalado nas estações de trabalho.
96. Os usuários de notebooks, smartphones e tablet que executam trabalho externo deverão sempre que retornar à Coopercredi realizar uma varredura em todos os discos rígidos e nos periféricos externos utilizados, garantindo que o seu equipamento não esteja contaminado e se estiver que não contamine toda a rede.
97. Nos casos em que for identificada contaminação intencional ou não por arquivos gravados colaboradores, a Unidade Adminitrativa informará o gestor da área para que tome as providências cabíveis.

DAS PENALIDADES

98. O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

DECLARAÇÃO DE COMPROMETIMENTO DA DIRETORIA EXECUTIVA

99. A Diretoria Executiva da Coopercredi ACSC declara-se comprometida em proteger todos os ativos ligados à Tecnologia da Informação, apoiando as metas e princípios da segurança da informação estabelecidas neste documento, a fim de garantir a confiabilidade, disponibilidade e integridade da informação alinhada com as estratégias do negócio.

VIGÊNCIA

100. Esta Política entrará em vigor a partir de 27 de junho de 2017 e vigorará por prazo indeterminado.